Recent uses and problems on Boolean and vectorial functions

Claude Carlet
University of Bergen
LAGA, University of Paris 8

We shall present a chapter in a forthcoming book on Boolean and vectorial functions, which is devoted to topics in this domain which emerged recently:

1. Physical attacks and related problems on functions and codes (a new role of correlation immunity and of the dual distance of codes related to side channel attack countermeasures, minimizing the number of nonlinear multiplications for reducing the cost of countermeasures, vectorial functions and threshold implementation, linear complementary dual codes and complementary pairs of codes used for direct sum masking, robust codes, algebraic manipulation detection AMD codes),

2. Fully homomorphic encryption and related questions on Boolean functions (with restricted inputs),

3. Local pseudorandom generators (the Goldreich pseudorandom generator) and related criteria on Boolean functions,

4. The Gowers norm on pseudo-Boolean functions.